Apache Tomcat: AJP secret compared in non-constant time

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43514
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 16:16:18 UTC
Updated	2026-05-12 18:17:27 UTC
Description	Observable Timing Discrepancy vulnerability when comparing AJP secret in Apache Tomcat. This issue affects Apache Tor

Risk And Classification

Problem Types: CWE-208 | CWE-208 CWE-208 Observable Timing Discrepancy

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 11.0.0-M1 11.0.21 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 10.1.0-M1 10.1.54 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.0.M1 9.0.117 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 8.5.0 8.5.100 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 7.0.0 7.0.109 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	unknown 7.00 semver	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/05/12/10	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
lists.apache.org/thread/2k654v5cq123npfsd1b2kk1y30owqb1m	security@apache.org	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**